IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

SCOTT PHILLIPS, on behalf of his minor son; and BELLVINIA BRICKLE, individually and on behalf of all others similarly situated, Plaintiffs, v. NextGen Healthcare Inc., Defendant.	Case No.: **JURY TRIAL DEMANDED** **COMPLAINT-CLASS ACTION**

CLASS ACTION COMPLAINT

Plaintiffs Scott Phillips, on behalf of his minor son, and Bellvinia Brickle (collectively "Plaintiffs"), individually and on behalf of all persons similarly situated (the "Class" or "Class Members"), by and through the undersigned counsel, bring this class action complaint against Defendant NextGen Healthcare Inc. ("NextGen" or "Defendant"). Plaintiffs make the following allegations based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Plaintiffs bring this class action against NextGen for its failure to secure and safeguard patients' personally identifiable information ("PII")[1] and for failing to provide timely, accurate, and adequate notice to Plaintiffs and Class Members that their PII had been compromised.

2. NextGen is a Georgia-based healthcare technology company that contracts with healthcare providers to deliver electronic health records software and practice management systems.[2] Healthcare providers entrust NextGen with sensitive patient information as part of using NextGen's services. Plaintiffs and Class Members are third-party beneficiaries to the promises made by NextGen to healthcare providers.

3. On April 28, 2023, NextGen began notifying state attorneys general and patients that it had sustained a massive data breach in which a hacker gained unauthorized access to its networks between at least March 29, 2023, and April 14, 2023 (the "Data Breach").[3]

---

[1] PII is information that is used to confirm an individual's identity, and in this instance includes at least an individual's name, address, email address, phone number, and Social Security number.

[2] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 4, 2023).

[3] Of note, although NextGen has stated it believes the data breach to be contained, NextGen has not confirmed that the incident actually is contained or that the data

4. NextGen admits the hacker accessed and acquired highly-sensitive information stored on NextGen's servers, including patient name, date of birth, address, and social security number.[4]

5. NextGen admits that the hacker "accessed the NextGen Office system by using NextGen client credentials that appear to have been stolen from sources or incidents unrelated to NextGen."[5]

6. NextGen admits the Data Breach has compromised the PII of more than one million patients.[6]

7. According to NextGen, the Data Breach started on March 29, 2023, and was discovered on March 30, 2023. But NextGen was unable to stop the breach until April 14, 2023, at the earliest. NextGen's notification letter is not clear that April 14,

---

breach has ended.

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 8, 2023).

[5] https://www.iowaattorneygeneral.gov/media/cms/522023_NextGen_86BD44F1E67CD.pdf (last visited May 5, 2023). This is the exact scenario contemplated in NextGen's 10-k filing: "We rely upon our clients as users of our system for key activities to promote security of the system and the data within it, such as administration of client-side access credentialing and control of client-side display of data. On occasion, our clients have failed to perform these activities. Failure of clients to perform these activities may result in claims against us that this reliance was misplaced, which could expose us to significant expense and harm to our reputation even though our policy is to enter into business associate agreements with our clients."

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 6, 2023).

2023, was when the breach was finally stopped.

8. Despite learning of the Data Breach on March 30, 2023, NextGen failed to inform the public of the Data Breach until nearly a month later on April 28, 2023.

9. The Data Breach occurred and was exacerbated because NextGen negligently failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

10. As a result of NextGen's failure to protect the sensitive information it was entrusted to safeguard, Plaintiffs and Class members have already suffered harm and have been exposed to a significant and continuing risk of identity theft, financial fraud, and other identity-related fraud for years to come.

PARTIES

11. Defendant NextGen Healthcare Inc. is a Delaware corporation registered with the state of Georgia as a Foreign Profit Corporation with its principal place of business at 3525 Piedmont Rd., NE, Building 6, Suite 700, Atlanta, Georgia 30305.

12. Plaintiff Scott Phillips and his minor son are residents and citizens of Galloway, New Jersey. On or about April 28, 2023, Mr. Phillips was notified via letter from NextGen dated April 28, 2023, that his son is a victim of the Data Breach.

13. Plaintiff Bellvinia Brickle is a resident and citizen of Philadelphia, Pennsylvania. On or about May 4, 2023, Ms. Brickle was notified via letter from NextGen dated April 28, 2023, that she was a victim of the Data Breach.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists because NextGen and at least one Class Member are citizens of different States. This Court also has supplemental jurisdiction over the claims in this case pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy under Article III of the United States Constitution.

15. The Court has personal jurisdiction over NextGen because NextGen is headquartered in Atlanta, Georgia and is thus essentially at home there. NextGen also conducts substantial business in Georgia related to Plaintiffs and Class Members and has thereby established minimum contacts with Georgia sufficient to authorize this Court's exercise of jurisdiction over NextGen.

16. Venue in the Northern District of Georgia is proper under 28 U.S.C. § 1391 because NextGen resides in this District, and a substantial part of the conduct

giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

FACTUAL ALLEGATIONS

NextGen's Privacy Practices

17. NextGen is a healthcare technology company that "provides electronic health records and practice management solutions to doctors and medical professionals."[7] NextGen holds itself out as "a leading provider of innovative, cloud-based, healthcare technology solutions that empower healthcare practices to manage the risk and complexity of delivering care in the United States healthcare system."[8]

18. NextGen recognizes the importance of data security: "If our security measures are breached or fail and unauthorized access is obtained to a client's data, our services may be perceived as not being secure, clients may curtail or stop using our services, and we may incur significant liabilities."[9] NextGen highlights its data security practices to potential healthcare provider customers.[10] NextGen advertises its data security to these customers promising: "We go to extraordinary lengths to

[7] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).
[8] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).
[9] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 4, 2023).
[10] https://www.nextgen.com/solutions/data-platforms (last visited May 4, 2023).

make your data as secure as possible . . . ."[11]

19. In the course of providing services, NextGen collects patients' highly sensitive PII, including Social Security numbers. As a result, these patients' highly sensitive PII is stored on NextGen's under-secured internet-accessible network.

20. In its 2022 Form 10-K, NextGen acknowledged the sensitivity and importance of this PII, their obligation to protect patients' PII, and the risks associated with failing to do so: "Our services involve the storage, transmission and processing of clients' proprietary information and protected health information of patients. Because of the sensitivity of this information, security features of our software are very important."[12]

21. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, NextGen assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from unauthorized disclosure.

22. NextGen maintains a privacy policy dated December 2022, that is accessible from its website ("Privacy Policy"). NextGen's Privacy Policy states that "[w]e use reasonably and appropriate security measures designed to protect the personal information we obtain from unauthorized alteration, loss, disclosure, or use,

[11] https://www.nextgen.com/services/managed-cloud (last visited May 4, 2023).
[12] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).

including technological, physical and administrative controls over access to systems we use to provide the Company Site and our products and services."[13] NextGen failed to comply with its privacy policy, thereby exposing patients' most sensitive personal information in the Data Breach.

The Data Breach

23. Between at least March 2022, and April 14, 2023, a hacker infiltrated NextGen's network and accessed a massive amount of highly sensitive PII stored on its servers, including full names and Social Security numbers of patients.

24. NextGen discovered the existence of the Data Breach on March 30, 2023, but did not disclose the Data Breach until nearly a month after its discovery, when it began notifying state attorneys general and affected borrowers on April 28, 2023.

25. In its notice to state attorneys general, NextGen stated:

a. The breach occurred on March 29, 2022;

b. It discovered the breach on March 30, 2023;

c. NextGen described the breach as "an unknown third-party gained unauthorized access to a limited set of electronically stored personal information"; and

[13] https://www.nextgen.com/privacy-policy (last visited May 4, 2023).

d. The hackers acquired Name or Other PII and Social Security numbers of over one million patients.[14]

26. NextGen's sample form notification letter provides the following description:

> On March 30, 2023, we were alerted to suspicious activity on our NextGen Office system. In response, we launched an investigation with the help of third-party forensic experts. We also took measures to contain the incident, including resetting passwords, and contacted law enforcement. Based on our in-depth investigation to date, supported by our external experts, it appears that an unknown third-party gained unauthorized access to a limited set of electronically stored personal information between March 29, 2023 and April 14, 2023. As a result of our detailed analysis of the information impacted, we recently determined that certain of your personal information was included in the electronic data accessed during the incident. Below we have provided information about what information was involved, what we are doing in response, and what you can do to proactively protect yourself.[15]

27. From NextGen's notice it is unclear exactly when information was taken; when NextGen "launched an investigation"; the total extent of what data was exposed; when NextGen took action to stop the breach; and whether the breach has actually been stopped.

28. The only meaningful information NextGen's notice provides is that all

---

[14] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023); https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last visited May 6, 2023).

[15] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last downloaded May 4, 2023).

or nearly all of the information provided by patients was compromised.

29. NextGen's notice also discusses actions NextGen claims to have taken in response to the Data Breach, stating, "[w]e also took measures to contain the incident, including resetting passwords, and contacted law enforcement."[16]

30. Absent from the notice are any details of how the Data Breach happened or how NextGen's actions may have remediated the root cause of the Data Breach.

31. NextGen has not posted an alert relating to the Data Breach on its website.[17]

32. NextGen provides no explanation for why it delayed notifying patients about the Data Breach for almost a month after it detected the Data Breach. The PII of Plaintiffs and Class Members could have been in the hands of hackers for nearly a month before NextGen attempted to notify affected patients. By waiting this long to disclose the Data Breach and by downplaying the risk that victims' PII would be misused by bad actors, NextGen prevented victims from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

The Data Breach was Preventable

[16] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).
[17] https://www.nextgen.com/ (last visited May 6, 2023).

33. In response to the Data Breach, NextGen stated it "launched an investigation with the help of third-party forensic experts."[18]

34. But NextGen, like any company of its size that stores massive amounts of sensitive personal and medical information, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to over one million patient files. NextGen's only disclosed tangible response to the Data Breach was to "reset[] passwords." If the Data Breach was so easily contained or remediated, NextGen's failure to prevent the breach is inexcusable given its knowledge that it was a prime target for cyberattacks.

35. Its status as a prime target for cyberattacks was known and obvious to NextGen as it disclosed in its own regulatory filings.[19] NextGen understood that the type of information it collects, maintains, and stores is highly coveted and a frequent target of hackers.

36. In its 2022 form 10-K NextGen acknowledged this danger:

> High-profile security breaches at other companies have increased in recent years, and security industry experts and government officials have warned about the risks of hackers and cyber-attacks targeting information technology products and businesses. Although this is an industry-wide problem that affects other software and hardware companies, we may be targeted by

[18] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).
[19] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last downloaded May 4, 2023).

> computer hackers because we are a prominent healthcare information technology company and have high profile clients. These risks will increase as we continue to … store and process increasingly large amounts of our client's confidential data, including personal health information…. Moreover, unauthorized access, use or disclosure of such sensitive information, including any resulting from the incidents described above, could result in civil or criminal liability or regulatory action, including potential fines and penalties. … These types of security incidents could also lead to lawsuits, regulatory investigations and claims, and increased legal liability.[20]

37. NextGen was keenly aware of its status as a prime target because it had in fact been victimized earlier this year. In January 2023, NextGen was the victim of a ransomware attack.[21] In response to this attack NextGen issued a statement including the following: "The privacy and security of our client information is of the utmost importance to us."[22]

38. In August 2018, NextGen's current Chief Information and Security Officer, David Slazyk, published a blog post on NextGen's website titled "Two essential ways to make your practice data more secure."[23] That blog post on NextGen's website is currently defunct. However, the article is still available on the

[20] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last visited May 5, 2023).
[21] https://www.washingtonpost.com/politics/2023/01/23/latest-cyberattack-health-care-shows-how-vulnerable-sector-is/ (last visited May 5, 2023).
[22] *Id.*
[23] https://www.nextgen.com/blog/make-your-practice-data-more-secure (last visited May 5, 2023).

internet archive.[24] In that blog post Mr. Slazyk acknowledged that "You have good reason to be concerned about the security of your practice's data. The last three years saw 955 major security breaches in healthcare, leading to exposure or theft of more than 135 million healthcare records and affecting more than 41 percent of the U.S. population."[25]

39. In that same blog post Mr. Slazyk represented that "At NextGen Healthcare we are committed to … Using the most advanced security controls available…"[26] He also represented that healthcare practices "can off-load the task of data protection to NextGen Healthcare by taking advantage of our hosting services."[27]

40. Data breaches and the harm they cause have become so common and notorious the Federal Trade Commission ("FTC") has issued guidance for how to address the destruction caused by an unauthorized person having access to someone's PII, warning: "Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility

---

24 https://web.archive.org/web/20211019184725/https://www.nextgen.com/blog/make-your-practice-data-more-secure (last visited May 5, 2023).

25 *Id.*

26 *Id.*

27 *Id.*

accounts, or get medical treatment on your health insurance."[28]

41. At all relevant times, NextGen knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individual patients as a result of a breach.

42. NextGen was, or should have been, fully aware of the significant number of patients whose PII it collected, and thus, the significant number of patients who would be harmed by a breach of its systems.

43. But despite all of the publicly available knowledge of the continued compromises of PII and despite holding the PII of millions of patients, NextGen failed to use reasonable care in maintaining the privacy and security of the PII of Plaintiffs and Class Members. Had NextGen implemented common sense security measures, hackers never could have accessed the PII of over one million patients and the Data Breach would have been prevented or much smaller in scope.

NextGen Failed to Comply with Federal Law and Regulatory Guidance

44. Federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For

[28] https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last accessed May 4, 2023).

example, the Federal Trade Commission (FTC) has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[29]

45. The FTC's publication Protecting Personal Information: A Guide for Business sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[30] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[31]

46. Additionally, the FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-

[29] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 4, 2023).
[30] *Id.*
[31] *Id.*

tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[32] This is consistent with guidance provided by the FBI.

47. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[33]

48. NextGen was fully aware of its obligation to implement and use reasonable measures to protect patients' PII but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. NextGen's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Defendant also failed to meet the minimum standards of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework Version

---

[32] *Id.*

[33] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited May 4, 2023).

1.1.[34]

Allegations Relating to Plaintiff Scott Phillips' Minor Son

50. Unbeknownst to Plaintiff Phillips, NextGen obtained Plaintiff's minor son's PII through one of NextGen's healthcare clients. At this time it is unclear which healthcare provider provided Plaintiff's minor son's PII to NextGen.

51. On or about April 28, 2023, Plaintiff received a notification letter from NextGen stating that his nine-year-old son was a victim of the Data Breach.

52. The letter recommended that Plaintiff take certain actions like monitoring his son's accounts and "remain vigilant by reviewing your account statements and credit reports closely."[35]

53. Despite making these recommendations, NextGen itself was not vigilant against the risks of a data breach.

54. To protect from additional harm, Plaintiff's minor son has been and will continue to be forced to spend significant time and effort engaging in remedial efforts to protect his son's information from additional attacks. Plaintiff must now continue to spend time and effort reviewing his son's credit profile and other

[34] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed May 4, 2023)
[35] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).

financial information and accounts for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff suffered significant distress knowing his son's highly personal information is no longer confidential and his son's accounts are being targeted. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff's son faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

55. Upon information and belief, NextGen continues to store Plaintiff's minor son's PII on its internal systems. Thus, Plaintiff has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

Allegations Relating to Plaintiff Bellvinia Brickle

56. Unbeknownst to Plaintiff Brickle, NextGen obtained Plaintiff Brickle's PII through one of NextGen's healthcare clients. At this time it is unclear which healthcare provider provided Plaintiff Brickle's PII to NextGen.

57. On or about May 4, 2023, Plaintiff Brickle received a notification letter from NextGen stating that she was a victim of the Data Breach.

58. The letter recommended that Plaintiff Brickle take certain actions like monitoring her accounts and "remain vigilant by reviewing your account statements

and credit reports closely."[36]

59. Despite making these recommendations, NextGen itself was not vigilant against the risks of a data breach.

60. To protect from additional harm, Plaintiff Brickle has been and will continue to be forced to spend significant time and effort engaging in remedial efforts to protect her information from additional attacks. Plaintiff Brickle must now continue to spend time and effort reviewing her credit profile and financial and other account statements for evidence of unauthorized activity, which she will continue to do indefinitely. Plaintiff Brickle suffered significant distress knowing her highly personal information is no longer confidential and her accounts are being targeted. Given the nature of the information exposed in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff Brickle faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

61. Upon information and belief, NextGen continues to store Plaintiff Brickle's PII on its internal systems. Thus, Plaintiff Brickle has a continuing interest

[36] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last visited May 4, 2023).

in ensuring that the PII is protected and safeguarded from future breaches.

The Impact of the Data Breach on Victims

62. NextGen's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, date of birth, and Social Security numbers—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

63. The PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities." [37]

[37] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

64. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

65. Victims of the Data Breach face significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Class Members are forced to spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

66. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% report problems with family members as a result of the breach;

- 10% reported feeling suicidal.[38]

67. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[39]

68. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[40]

---

[38] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited May 4, 2023).

[39] https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited May 4, 2023).

[40] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

69. Plaintiffs are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

70. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the inherent value of their PII;

c. losing the value of access to their PII permitted by NextGen;

d. identity theft and fraud resulting from the theft of their PII;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

g. the present value of ongoing credit monitoring and identity theft protection services necessitated by NextGen's Data Breach;

h. unauthorized charges and loss of use of and access to their accounts;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or many unauthorized third parties.

71. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

72. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the

harm resulting from data breaches cannot necessarily rule out all future harm."[41]

73. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[42]

74. Likewise, the American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a data breach, with 63% of consumers indicating they would avoid such a company for a period of time.[43]

75. Plaintiffs and Class Members have an interest in NextGen's promises and duties to protect the PII they entrusted to healthcare providers, *i.e.*, that NextGen

---

[41] http://www.gao.gov/new.items/d07737.pdf (last visited May 4, 2023).

[42] https://web.archive.org/web/20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited May 4, 2023).

[43] https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/ (last visited May 4, 2023).

not increase their risk of identity theft and fraud. Because NextGen failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by NextGen's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have occupied but for NextGen's wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' PII.

76. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII permitted through NextGen's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, Plaintiffs may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of

damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

77. NextGen's delayed notice letter also caused Plaintiffs and Class Members harm. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. NextGen's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting nearly a month to disclose the Data Breach and by downplaying the risk of misuse, NextGen prevented victims from taking meaningful, proactive, and targeted mitigation measures to secure their PII and accounts.

78. Plaintiffs and Class Members have an interest in ensuring that their PII is secured and not subject to further theft because NextGen continues to hold their PII.

CLASS ACTION ALLEGATIONS

79. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4),

Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

All individuals residing in the United States whose PII was compromised in the Data Breach.

80. The Class asserts claims against NextGen for negligence (Count I), unjust enrichment (Count II), invasion of privacy (Count III), and third-party beneficiary breach of contract (Count IV).

81. Specifically excluded from the Nationwide Class are NextGen and its officers, directors, or employees; any entity in which NextGen has a controlling interest; and any affiliate, legal representative, heir, or assign of NextGen. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

82. **Jurisdictional Amount.** As alleged herein, Plaintiffs seek damages on behalf of themselves and the over one million putative class members, satisfying the $5 million jurisdictional requirement of 28 U.S.C. § 1332(d)(2).

83. **Ascertainablity.** The members of the Class are readily identifiable and ascertainable. NextGen and/or its affiliates, among others, possess the information to identify and contact Class Members.

84. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members

of the Class are so numerous that joinder of all of them is impracticable. NextGen's statements reveal that the Class contains over one million individuals whose PII was compromised in the Data Breach.

85. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** As to the Class, Plaintiffs' claims are typical of the claims of the members because all Class Members had their PII compromised in the Data Breach and were harmed as a result.

86. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and their interests are aligned with Class Members' interests. Plaintiffs were subject to the same Data Breach as Class Members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases.

87. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

a. Whether NextGen owes Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and

practices to protect their PII;

b. Whether NextGen acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members' PII;

c. Whether NextGen violated its duty to implement reasonable security systems to protect Plaintiffs' and Class Members' PII;

d. Whether NextGen's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

e. Whether NextGen provided timely notice of the Data Breach to Plaintiffs and Class Members; and

f. Whether Plaintiffs and Class Members are entitled to compensatory damages, punitive damages, and/or nominal damages as a result of the Data Breach.

88. NextGen has engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by NextGen's failure to maintain reasonable security procedures and practices to protect patients' PII, as well as NextGen's failure to timely alert affected patients to the Data Breach.

89. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions

by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

90. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

91. Unbeknownst to Plaintiffs and Class Members, NextGen and/or its affiliates obtained their PII from healthcare providers for commercial gain. NextGen collected and stored this PII for purposes of providing services to its customers and their patients.

92. NextGen owed Plaintiffs and Class Members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access.

93. NextGen owed a duty of care to Plaintiffs and Class Members to provide adequate data security, consistent with industry standards, to ensure that NextGen's systems and networks adequately protected the PII.

94. NextGen's duty to use reasonable care in protecting PII arises as a result of the parties' relationship through healthcare providers, as well as common law and federal law, and NextGen's own policies and promises regarding privacy and data security. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices.

95. Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as NextGen, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

96. The FTC publications and orders described above also form part of the basis of NextGen's duty in this regard.

97. NextGen violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. NextGen's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class Members.

98. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

99. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

100. NextGen's violations of Section 5 of the FTC Act therefore constitute negligence *per se*.

101. NextGen knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location, NextGen's vulnerability to network attacks, and the importance of adequate security.

102. NextGen breached its duty to Plaintiffs and Class Members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class Members;

b. Failing to comply with industry standard data security measures leading up to the Data Breach;

c. Failing to comply with its own Privacy Policy;

d. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of NextGen's network and systems;

f. Failing to recognize in a timely manner that PII had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

103. Plaintiffs' and Class Members' PII would not have been compromised but for NextGen's wrongful and negligent breach of its duties.

104. NextGen's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access and exfiltration of PII by unauthorized third parties. Given that healthcare service providers are prime targets for hackers, Plaintiffs and Class Members are part of a foreseeable, discernible group that was at high risk of having their PII misused or disclosed if not adequately protected by NextGen.

105. It was also foreseeable that NextGen's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class Members.

106. As a direct and proximate result of NextGen's conduct, Plaintiffs and Class Members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and

recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in NextGen's possession and is subject to further unauthorized disclosures so long as NextGen fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by NextGen's data breach; and (x) any nominal damages that may be awarded.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

107. Plaintiffs repeat and reallege every allegation set forth in paragraphs 1 through 89.

108. Plaintiffs and Class Members have an interest, both equitable and legal,

in the PII about them that was conferred upon, collected by, used by, and maintained by NextGen and that was ultimately stolen in the NextGen data breach.

109. NextGen benefited by the conferral upon it of the PII pertaining to Plaintiffs and the Class Members and by its ability to retain, use, and profit from that information. NextGen understood and valued this benefit.

110. NextGen also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon NextGen maintaining the privacy and confidentiality of that PII.

111. Without NextGen's willingness and commitment to maintain the privacy and confidentiality of the PII, that PII would not have been transferred to and entrusted to NextGen. Further, if NextGen had disclosed that their data security measures were inadequate, they would not have been permitted to continue in operation by regulators or their clients.

112. NextGen admits that it uses the PII it collects for, among other things: "marketing and promotional communications."[44]

113. Because of NextGen's use of Plaintiffs' and Class Members' PII, NextGen sold more services and products than it otherwise would have. NextGen was unjustly enriched by profiting from the additional services and products it was

[44] https://www.nextgen.com/privacy-policy (last visited May 4, 2023).

able to market, sell, and create to the detriment of Plaintiffs and Class Members.

114. NextGen also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

115. NextGen also benefitted through its unjust conduct in the form of the profits it gained through the use of Plaintiffs' and Class Members' PII.

116. It is inequitable for NextGen to retain these benefits.

117. As a result of NextGen wrongful conduct as alleged in this Complaint (including among other things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), NextGen has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

118. NextGen's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

119. It is inequitable, unfair, and unjust for NextGen to retain these

wrongfully obtained benefits. NextGen's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

120. The benefit conferred upon, received, and enjoyed by NextGen was not conferred gratuitously, and it would be inequitable, unfair, and unjust for NextGen to retain the benefit.

121. NextGen's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their PII and has caused the Plaintiffs and Class Members other damages as described herein.

122. Plaintiffs and Class Members have no adequate remedy at law.

123. NextGen is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on NextGen as a result of its wrongful conduct, including specifically: the value to NextGen of the PII that was stolen in the Data Breach; the profits NextGen received and is receiving form the use of that information; the amounts that NextGen overcharged Plaintiffs and Class Members for use of NextGen's products and services; and the amounts that NextGen should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

124. Plaintiffs repeat and reallege every allegation set forth in paragraphs 1 through 89.

125. Plaintiffs and Class Members shared PII with NextGen and/or its affiliates that Plaintiffs and Class Members wanted to remain private and non-public.

126. Plaintiffs and Class Members reasonably expected that the PII they shared with NextGen would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

127. NextGen intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a criminal third party.

128. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, NextGen unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosures of their PII without consent.

129. The PII that was compromised during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other information that is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it.

130. NextGen's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

131. As a direct and proximate result of NextGen's invasion of privacy, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNTY IV
BREACH OF CONTRACTS OF WHICH PLAINTIFFS ARE THIRD PARTY BENEFICIARIES
(On behalf of Plaintiffs and the Class)

132. Plaintiffs repeat and reallege every allegation set forth in paragraphs 1 through 89.

133. Acting in the ordinary course of their business NextGen entered into

contracts with healthcare providers to deliver electronic health records software and practice management systems.

134. On information and belief, those respective contracts contained provisions requiring NextGen to protect the patient information that NextGen received in order to provide services to healthcare providers.

135. On information and belief, these provisions requiring NextGen acting in its ordinary course of business to protect personal information of the healthcare providers' patients was intentionally included for the direct benefit of Plaintiffs and Class Members, such that Plaintiffs and Class Members are intended third party beneficiaries of these contracts and are therefore entitled to enforce them.

136. NextGen breached these contracts while acting in the course of its business by not protecting Plaintiffs' and Class Members' PII, as stated herein.

137. As a direct and proximate result of NextGen's breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs

and their Counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit and prevent NextGen from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by NextGen as a result of their unlawful acts, omissions, and practices;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

F. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial in the instant action.

Dated: May 8, 2023

/s/ J. Cameron Tribble
Roy E. Barnes, Georgia Bar No. 03900
J. Cameron Tribble, Georgia Bar No. 754759
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: 770-227-6375
Fax: 770-227-6373
E-Mail: roy@barneslawgroup.com
E-Mail: ctribble@barneslawgroup.com

Norman E. Siegel,* Missouri Bar No. 44378
Barrett J. Vahle,* Missouri Bar No. 56674
J. Austin Moore, * Missouri Bar No. 64040
Tanner J. Edwards,* Missouri Bar No 68039
Brandi S. Spates,* Missouri Bar No 72144
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com
tanner@stuevesiegel.com
spates@stuevesiegel.com

Counsel for Plaintiffs

**Pro Hac Vice Forthcoming*